PRBIT - Princípy bezpečnosti informačných technológií

Report - Domáca úloha č.7

Autor: Marek Čederle

Cvičenie: Pondelok 17:00

Použité príkazy a ich vysvetlenie

Zadanie č.1

1. Na pridelenom virtuálnom PC – Windows Server sa prihláste poskytnutými údajmi do účtu Administrator.
2. *Vytvorte nový používateľský účet user1, ktorý bude pre bežného používateľa, heslo nastavte „Heslo123456“. Používateľ musí byť členom skupiny Users.
   Dokumentujte výpisom príkazov, z ktorých bude zrejmé, akí používatelia sú na Windows zriadení a akých skupín sú členmi.
3. Prihláste sa novým kontom user1 na server. Je prihlásenie povolené? Ak nie, prečo?
4. *Nastavte konto user1 do príslušných používateľských skupín tak, aby sa mohol daný používateľ prihlásiť interaktívne na server – v našom prípade postačuje cez vzdialenú pracovnú plochu.
   a. Dokumentujte snímkou obrazovky tak , aby bolo zrejmé, že používateľ user1 je prihlásený.
   b. Dokumentujte výpisom príkazov, ktoré zobrazia, akých skupín je používateľ user1 členom

2.

```
net user user1 Heslo123456 /add
```

Do skupiny `Users` je automaticky pridaný a vieme to overiť príkazom `net users user1`.

```
# PS C:\Users\Administrator> net users user1
User name                    user1
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            28. 10. 2024 17:28:19
Password expires             9. 12. 2024 17:28:19
Password changeable          28. 10. 2024 17:28:19
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.
```

Všetkých užívateľov môžeme zobraziť príkazom `net users`.

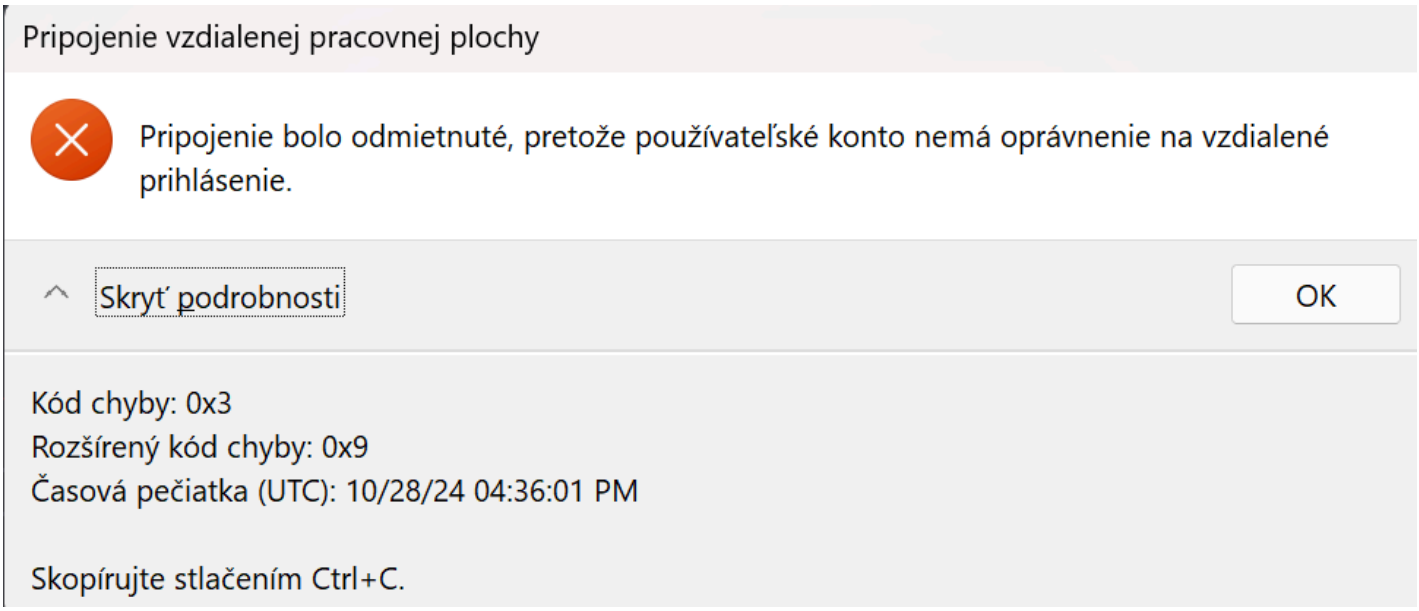
```
User accounts for \\WIN-STUDENT-6

-------------------------------------------------------------------------------
Admin                    Administrator            cloudbase-init
DefaultAccount           Guest                    user1
WDAGUtilityAccount
The command completed successfully.
```

Ak chceme zistiť skupinu každeého používateľa, vieme použiť príkaz, ktorý bol spomenutý vyššie ale nahradíme `user1` za iné používateľské meno.

3.

Nie, pretože na to nemá oprávnenie.

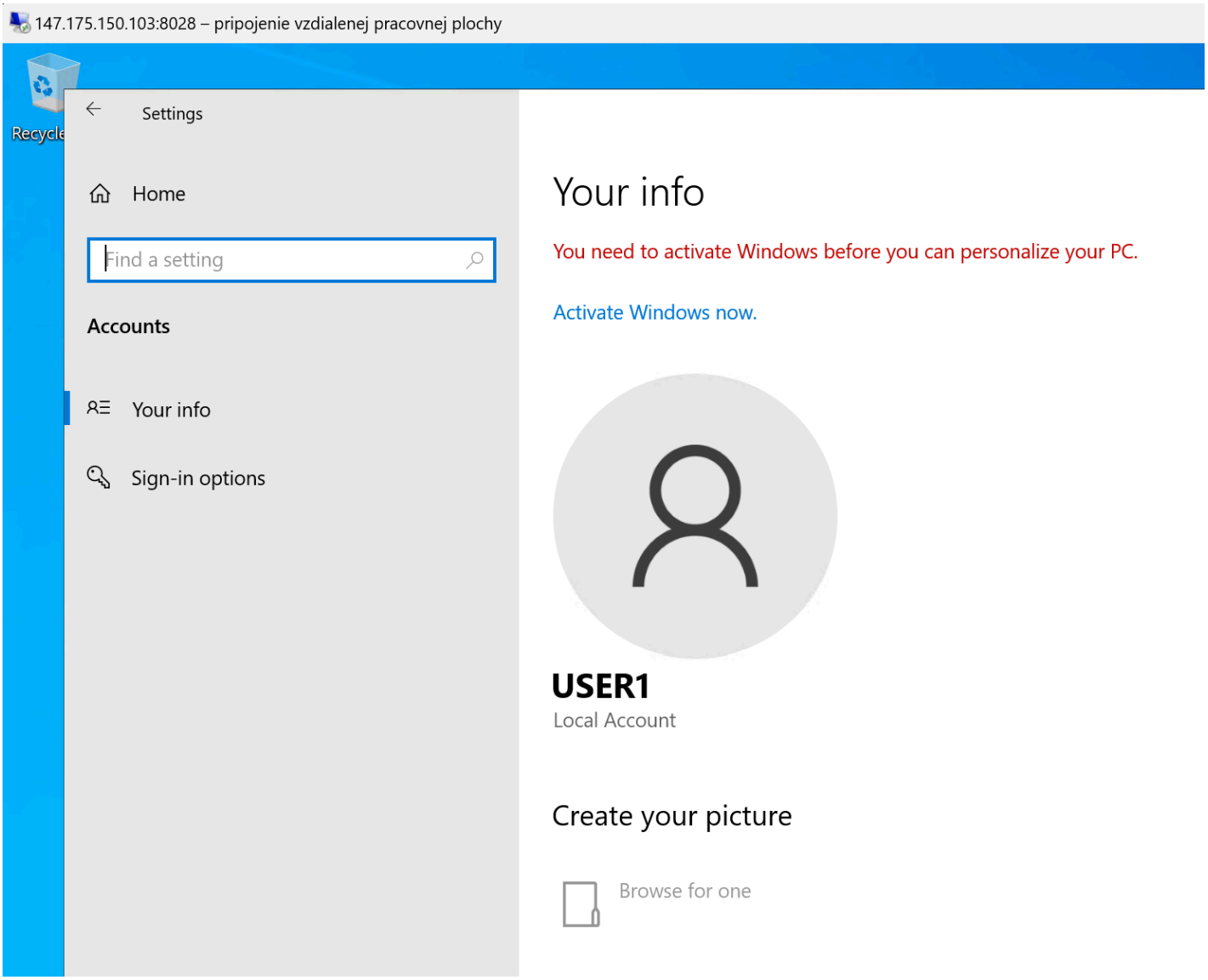


4.

Keď sa prihlásime znova ako administrátor, môžeme pridať používateľa do skupiny `Remote Desktop Users` príkazom:

```
net localgroup "Remote Desktop Users" user1 /add
```

- a)


147.175.150.103:8028 – pripojenie vzdialenej pracovnej plochy
Recycle
Settings
Home
Find a setting
Accounts
Your info
Sign-in options
Your info
You need to activate Windows before you can personalize your PC.
Activate Windows now.
USER1
Local Account
Create your picture
Browse for one

- b)

```
PS C:\Users\Administrator> net localgroup "Remote Desktop Users" user1 /add
The command completed successfully.

PS C:\Users\Administrator> net user user1
User name                    user1
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            28. 10. 2024 17:28:19
Password expires             9. 12. 2024 17:28:19
Password changeable          28. 10. 2024 17:28:19
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   28. 10. 2024 17:36:02

Logon hours allowed          All

Local Group Memberships      *Remote Desktop Users *Users
Global Group memberships     *None
The command completed successfully.
```

Zadanie č.2

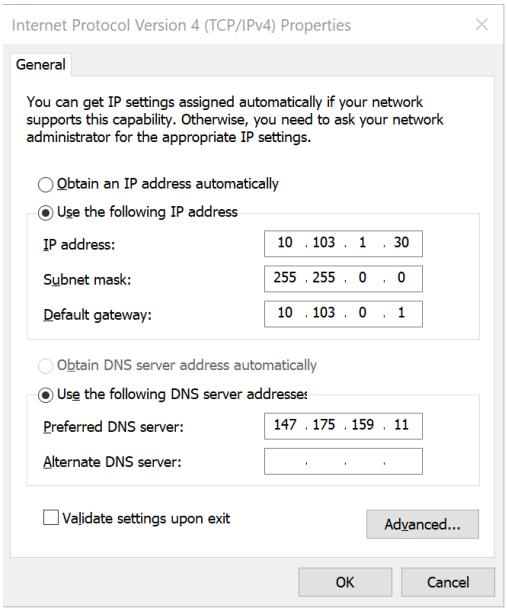
Vašou úlohou je zriadiť doménu Active Directory a „povýšiť“ Váš Windows server na radič domény/doménový kontrolór ADDC.

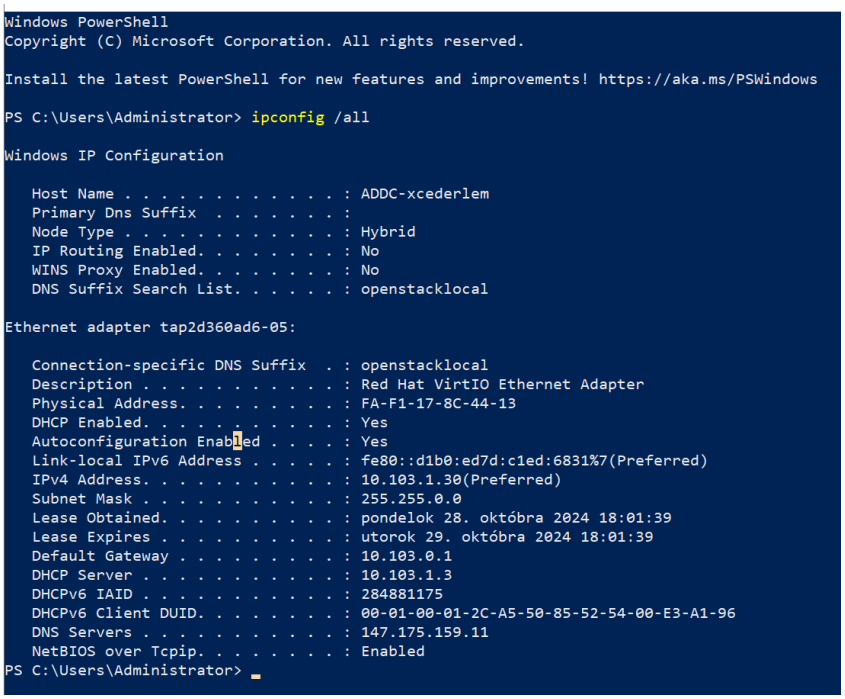
- Premenujte Váš server – zmeňte mu hostname na ADDC (dobrá prax, po vytvorení domény je zmena názvu hostname komplikovanejšia)

- Nastavte statickú IP adresu Vášmu serveru – zobrazte si aktuálne parametre siete a nastavte ich staticky – pretože nedá sa zriadiť doménový radič tak, aby mal IP adresu z DHCP (pretože na ADDC je súčasťou adresárovej služby aj DNS server)
- Nainštalujte rolu Active Directory Domain Services a DNS server.
- Povýšte Váš server na doménový radič a vytvorte novú doménu „vasemeno.local“, pričom za vasemeno **je nutné dosadiť Vaše krstné meno**. Riešenia s iným názvom domény než je Vaše krstné meno nebudú akceptované!
- Server sa na záver reštartuje. Prihláste sa naň.

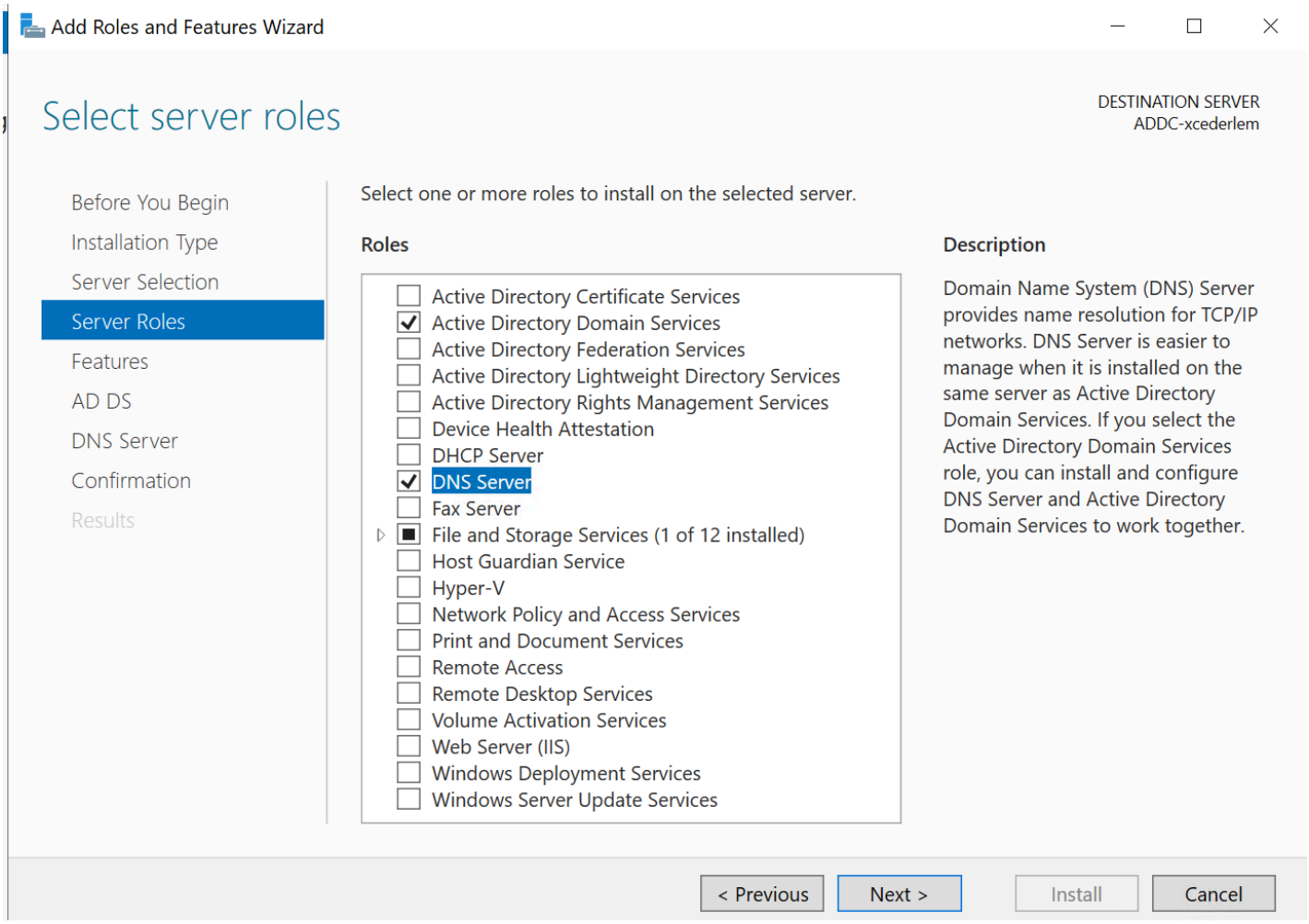
- Zmena mena na ADDC

- Nastavenie statickej IP adresy

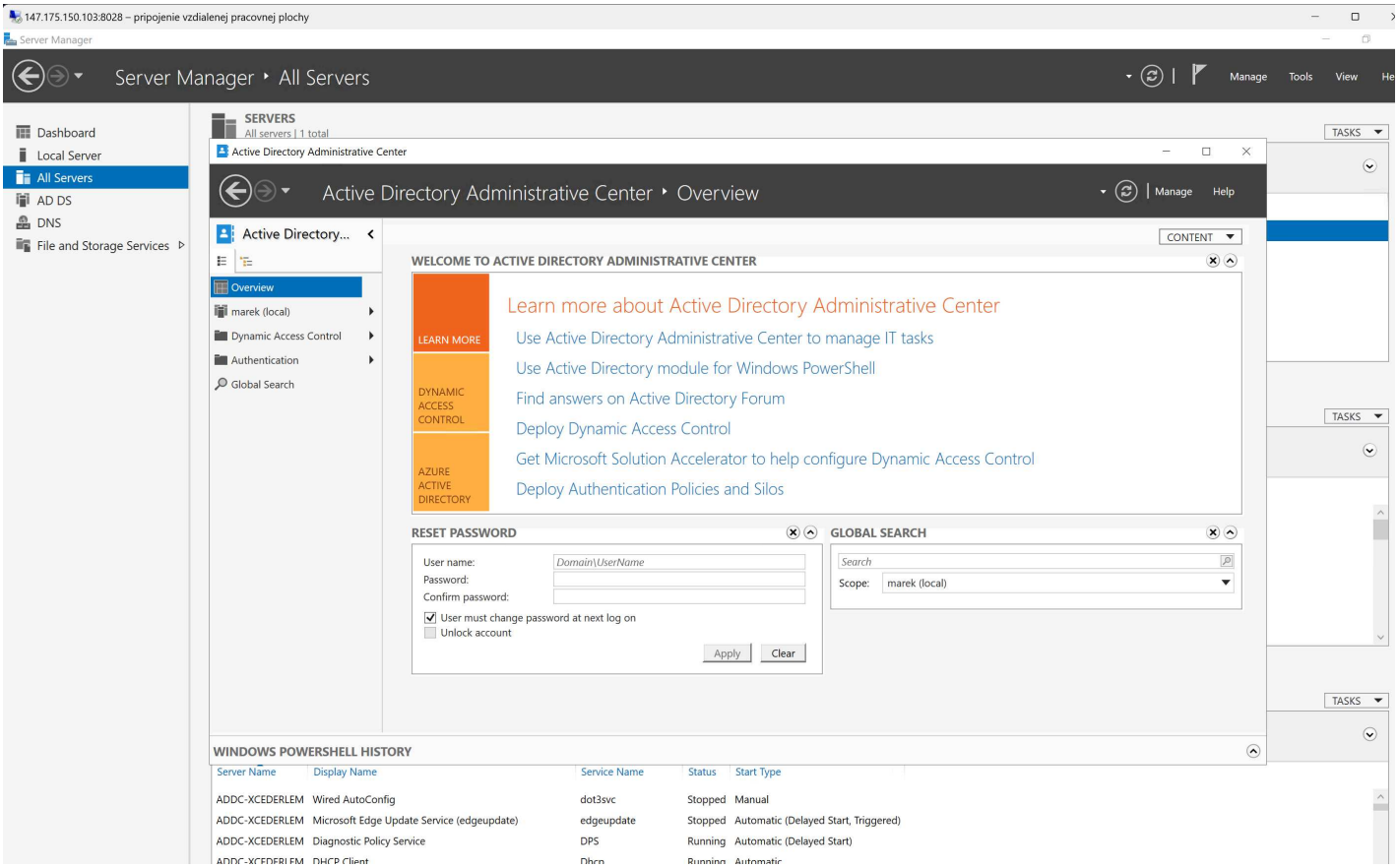




- Nainštalovanie Active Directory a DNS servera



- Úspešne nainštalovaný DNS a AD radič



Zadanie č.3

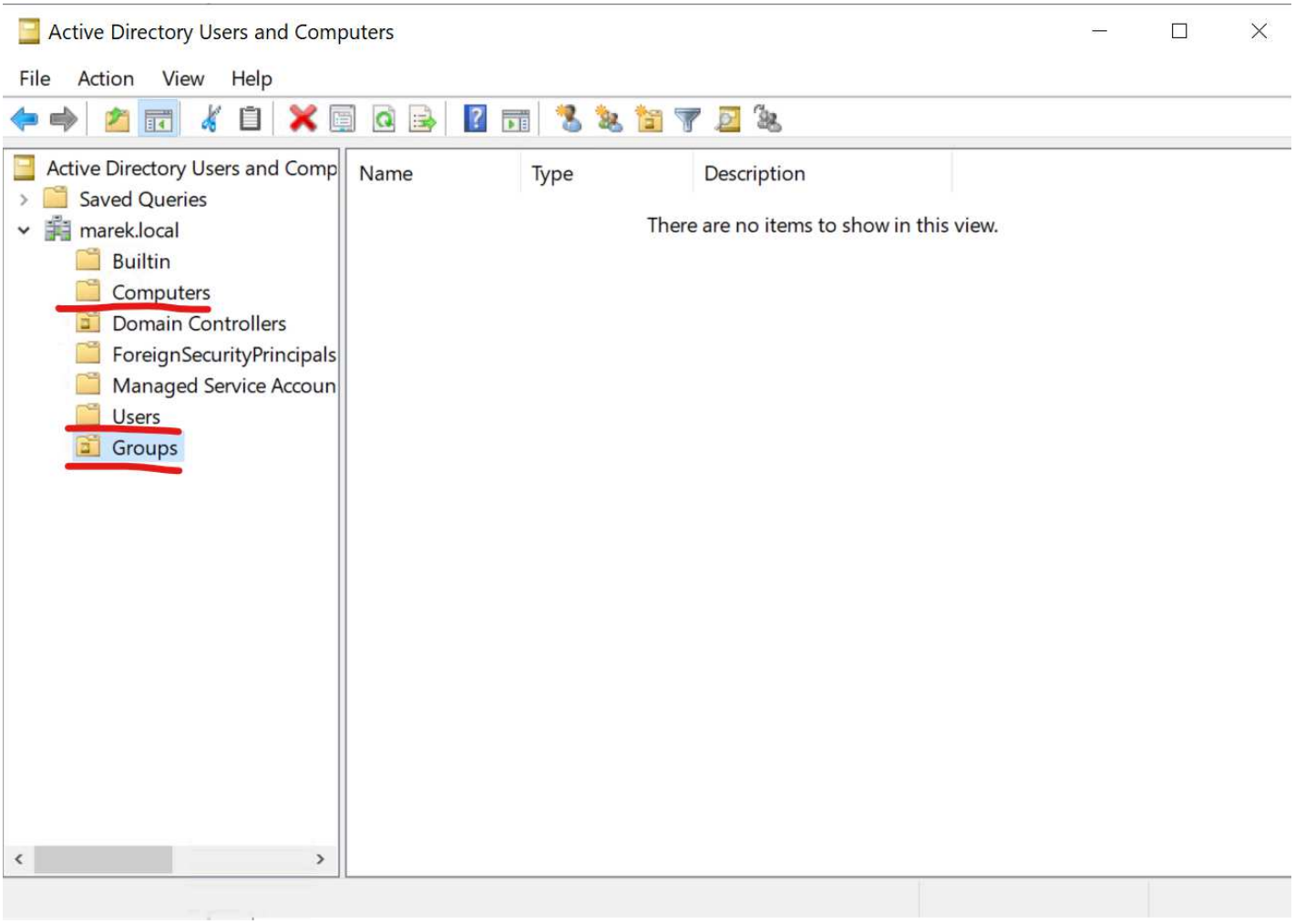
Úloha 3 - vytvorenie štruktúry domény a používateľa

Hodnotenie: 1 b

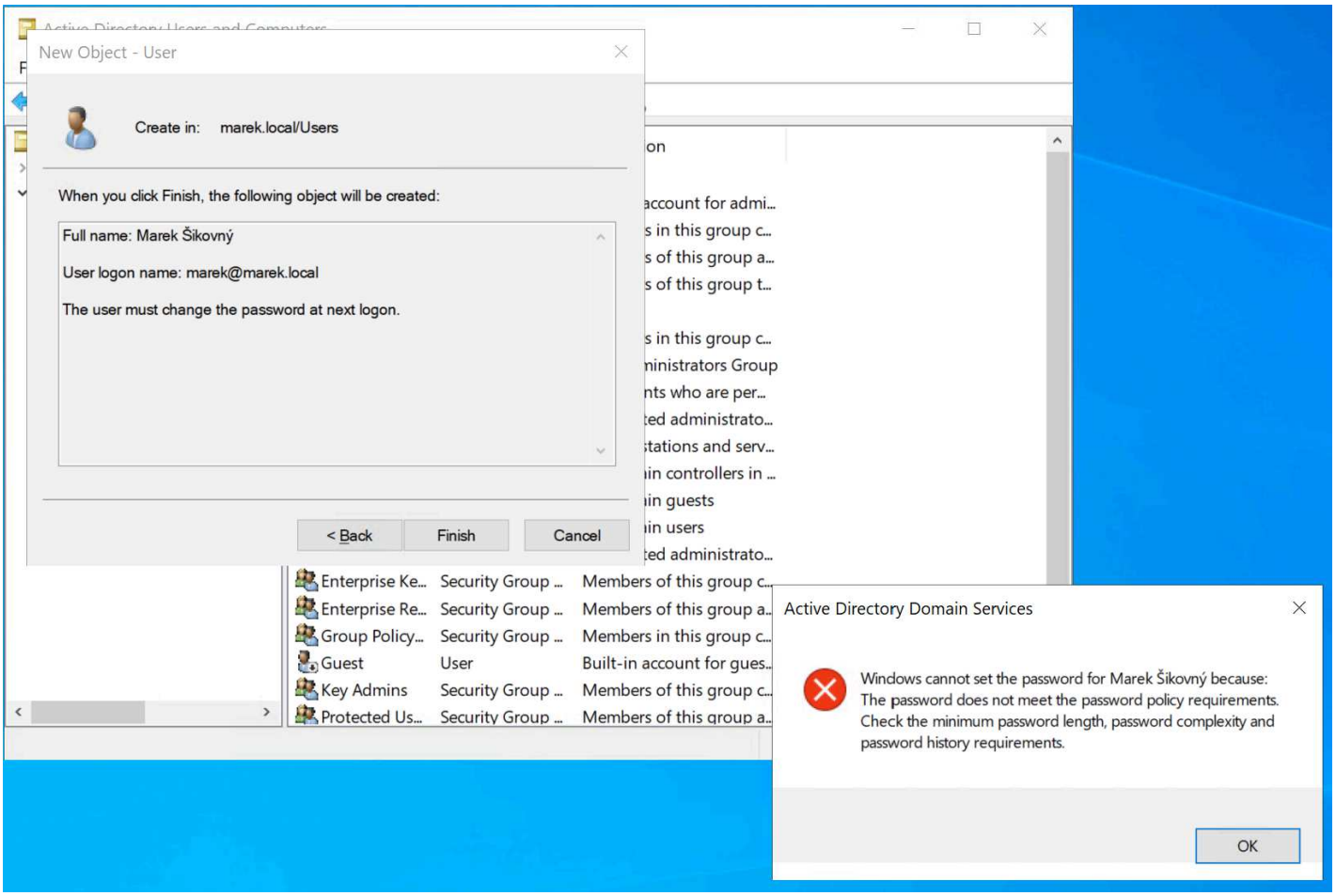
Svoj postup dokumentujte snímkami obrazovky a stručnými komentármi.

- Pomocou na to určených nástrojov (GUI či PowerShell moduly) vytvorte organizačnú štruktúru domény. Predovšetkým vytvorte organizačné jednotky pre používateľov, počítače a skupiny.
- Do organizačnej jednotky pridajte používateľa, ktorý bude mať login name Vaše krstné meno, meno – Vaše krstné meno, priezvisko – Šikovný. **Riešenia s iným menom než je Vaše krstné meno nebudú akceptované!**
  Heslo nastavte abc
- Systém Vám oznámi, že takéto heslo nie je možné akceptovať. Zistite, aká je aktuálne platná politika hesla na Vašom serveri a podľa toho vytvorte vlastné heslo, ktoré uvediete do riešenia, spolu so znením príslušnej politiky hesla. **Upozornenie – na každom z Windows Serverov je nastavená iná politika hesla.**
  Politiku hesla je možné zistiť rôznymi spôsobmi, pričom preferujeme v tomto prípade postup jej zistenia pomocou GUI. Pomôcka – pomocou GUI nenájdete nástroj „password policy“, také vo Windows neexistuje, ale tieto opatrenia sú špecifikované v rámci „celého balíka“ opatrení.

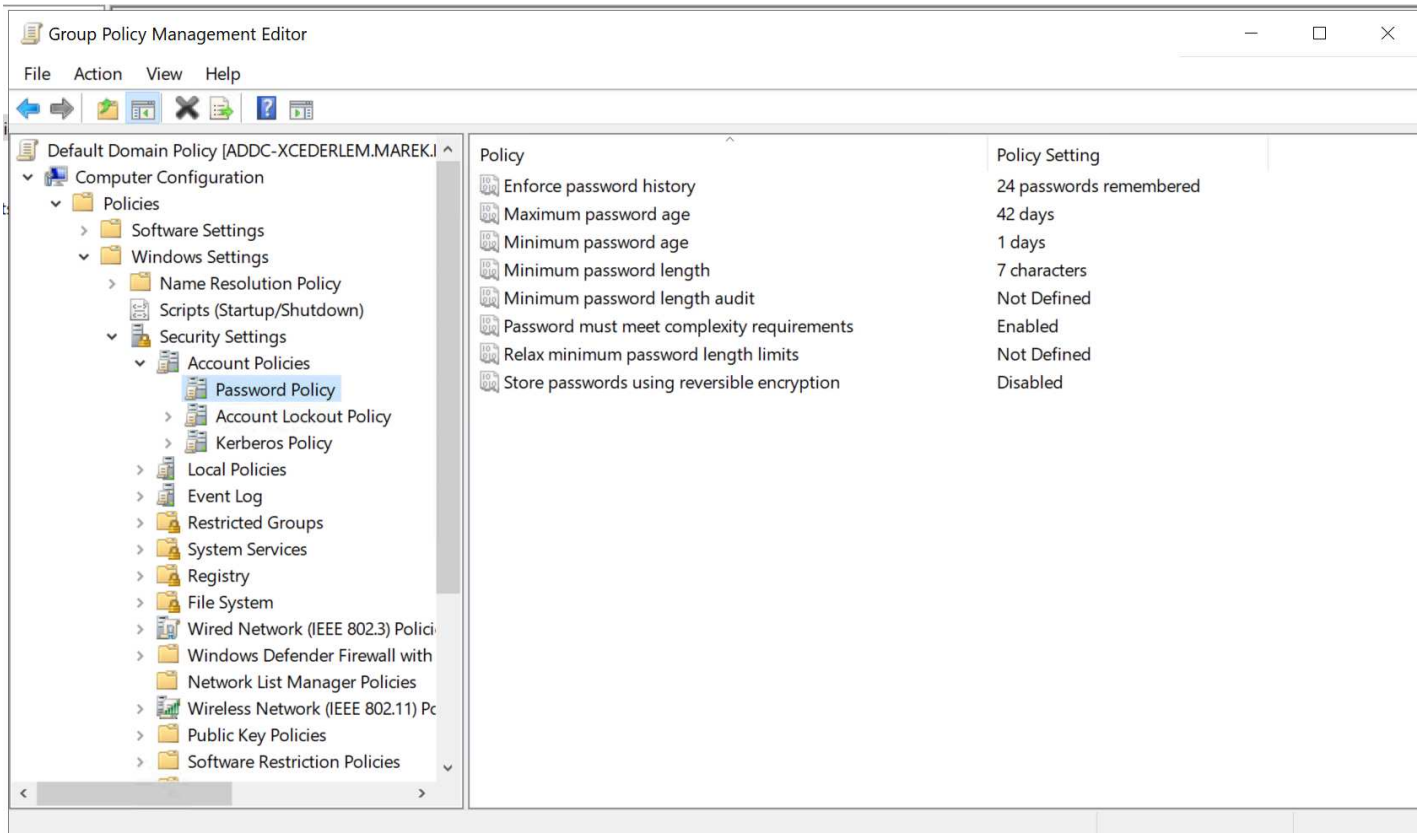
- Organizačné jednotky `Users` a `Computers` boli už vytvorené, takže som vytvoril už iba OU `Groups`.



- Vytvorenie používateľa



- Zistenie politík pre tvorbu hesla



- Heslo: `Xcederlem123*` Toto heslo spĺňa všetky požiadavky, ktoré sú nastavené v politike pre heslá.

Bonusové zadanie

1. Prostredníctvom skupinovej politiky nastavte odporúčané nastavenia Politiky hesla a zamykanie účtov. Riešenie je potrebné realizovať **vytvorením vlastného objektu skupinovej politiky tak, že samotný objekt skupinovej politiky sa musí volať „Poltika hesla – VaseKrstneMeno“**. Riešenia s politikou v názve neobsahujúcou Vaše krstné meno nebudú akceptované.

   Študijný materiál: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy
   Nastavte:
   - platnosť hesla jeden rok
   - minimálny vek hesla nedefinujte – resp. nastavte aby nebol vyžadovaný
   - dĺžka hesla 10 znakov
   - komplexita hesla – povoľte + stručne jednou vetou vysvetlite, aké znaky musí obsahovať heslo aby bolo v prostredí MS Windows považované za komplexné

   - nastavte zamknutie konta pri neúspešnom prihlasovaní nasledovne:

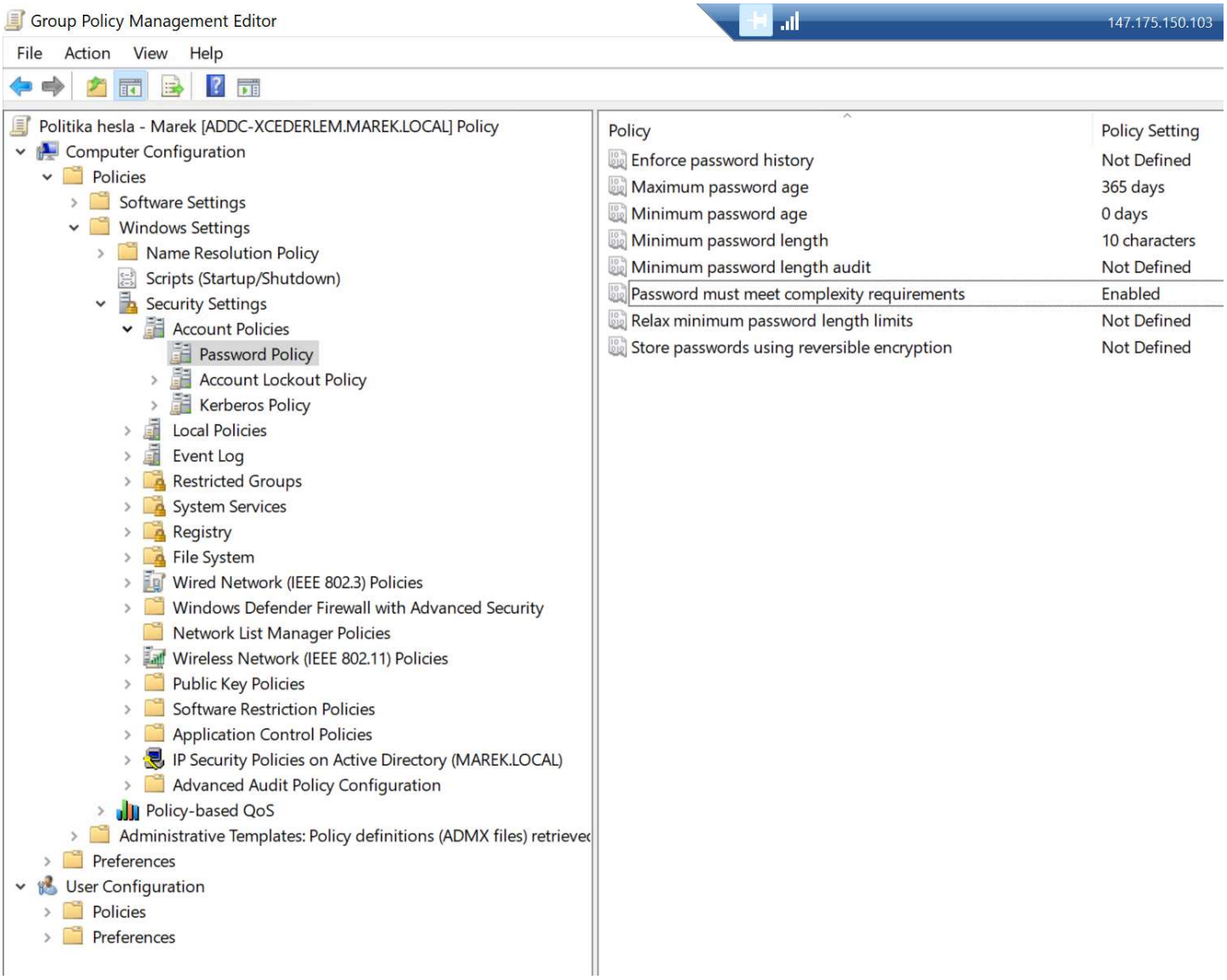
Account Policies/ Account Lockout Policy	
Policy	**Setting**
Account lockout duration	35 minutes
Account lockout threshold	7 invalid logon attempts
Reset account lockout counter after	35 minutes

2. Zistite, aký príkaz je potrebné použiť na to, aby sa zadefinované možnosti v politike aplikovali, prípadne zdôvodnite, či je potrebné reštartovať server.

3. Zdôvodnite, prečo je dôležité, aby bola stanovená Minimum password age, môžete ilustrovať na príklade. Nápoveda – berte do úvahy, že v podnikovom prostredí je heslo používateľa synchronizované pomocou adresárovej služby LDAP a používa sa na prihlásenie sa k Office365, AIS, interné informačné systémy, VPN, ...

4. Prostredníctvom printscreenov ukážte, kde je možné nastaviť v skupinovej politike voľbu vynútenia stláčania kombinácie kláves CTRL+ALT+DEL pri prihlasovaní sa do PC. Zároveň vysvetlite, prečo je vhodné toto nastavenie povoliť.

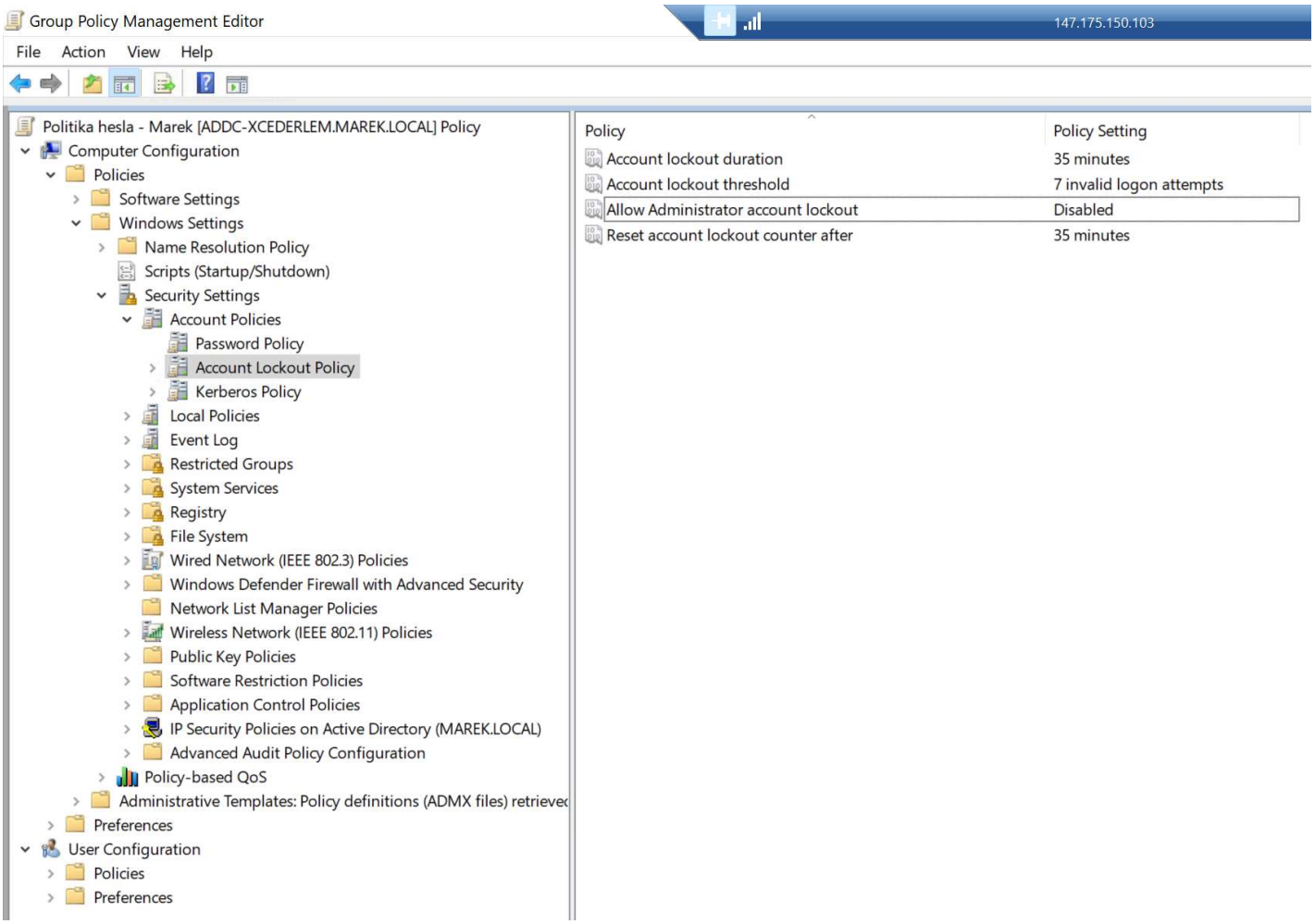
1.



Komplexné heslo musí spĺňať nasledujúce požiadavky:

- nesmie obsahovať meno používateľa alebo časti celého mena používateľa, ktoré presahujú dva po sebe idúce znaky
- mať dĺžku aspoň 6 znakov
- obsahovať znaky aspoň z troch z nasledujúcich štyroch kategórií:
- veľké anglické znaky (A až Z)
- a nglické malé písmená (a až z)
- číslice (0 až 9)
- nealfabetické znaky (napríklad !, $, #, %) (špeciálne znaky)

Nastavenie pre zamknutie účtu:



2.

```
gupdate /force
```

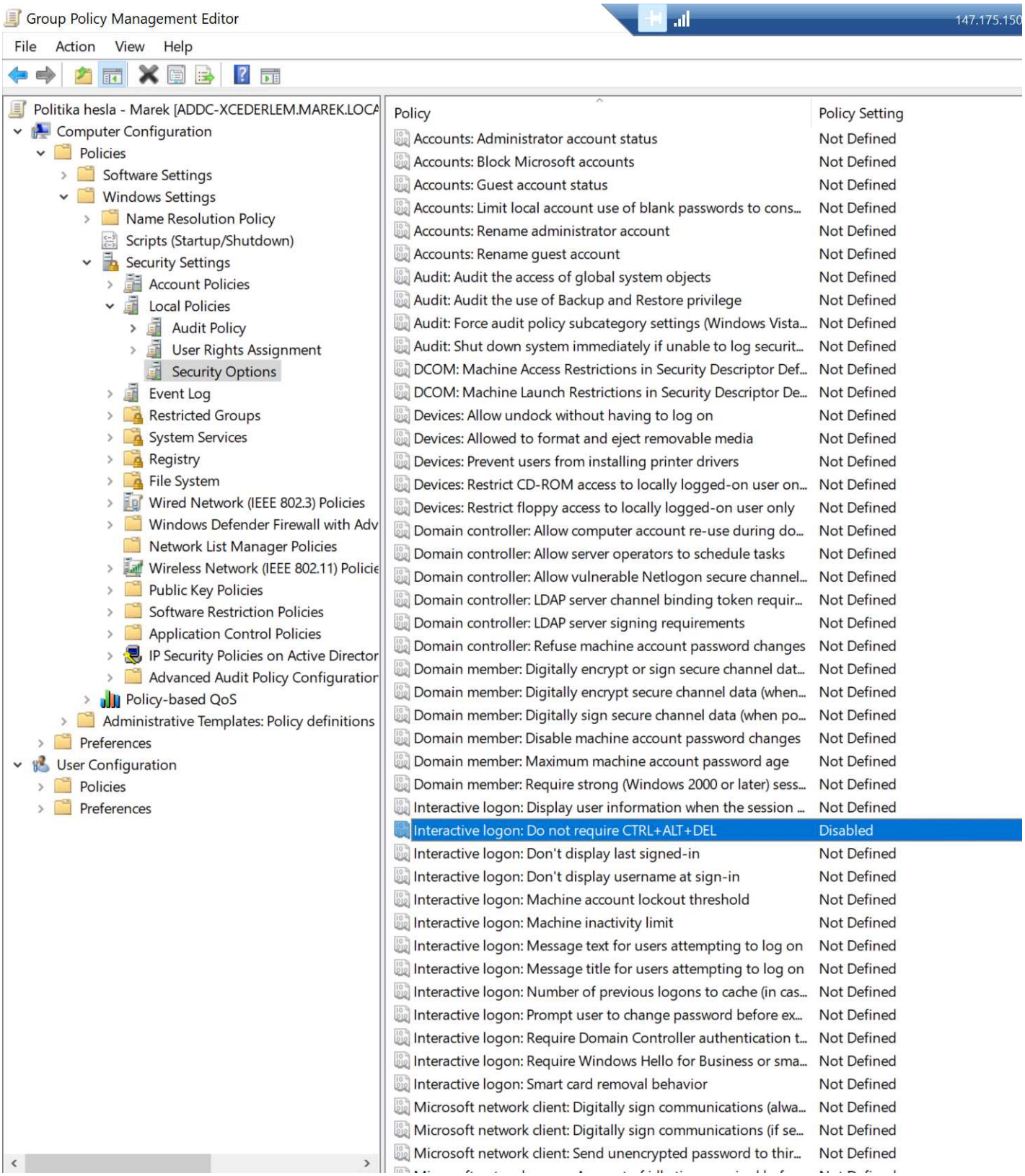
Príkaz spustí vynútenú aktualizáciu politík skupiny a aplikuje všetky politiky bez čakania na ďalšie plánované obnovenie.

V tomto prípade nie je treba reštartovať server, ale ak nám toto zlyhá z nejakého dôvodu (napr. nedostatočné oprávnenia a pod.), tak je vhodné reštartovať server.

3.

Bez `Minimal password age` by používatelia mohli rýchlo zmeniť svoje heslo niekoľkokrát za sebou, aby sa vrátili k pôvodnému heslu. Napríklad, ak je politika hesla nastavená tak, že heslo môže byť rovnaké až po 5 zmenách (t.z. pamätá si históriu hesiel), bez tejto politiky by používateľ by mohol zmeniť heslo 5-krát za sebou a vrátiť sa k pôvodnému heslu, čím by vedel obísť tieto bezpečnostné opatrenia. Ďalším dôvodom je, že v podnikovom prostredí, kde sa heslá nejako synchronizujú a používajú sa na prihlásenie do rôznych systémov, tak je dôležité, aby heslá zostali konzistentné po nejakú určitú dobu pretože by mohlo dôjsť ku nejakým problémom, že niekde by bolo heslo zmenené a niekde nie a nevedel by sa používateľ prihlásiť na danú službu.

4.



Skratka `CTRL+ALT+DEL` je kombinácia kláves, ktorá je určená pre systém a iba ten ju vie zachytiť. To znamená, že v prípade ak by na našom počítači bol nejaký malware, tak by nemohol zachytiť túto kombináciu klávesov (napr. nejaká phishing obrazovka, ktorá by sa tvárila ako daná obrazovka na zadávanie hesla), čo pre používateľa vzbuduje dôveru v daný systém a tvorí bezpečné prostredie.